PATENT ABSTRACTS OF JAPAN

(11)Publication number : **10-051440**
(43)Date of publication of application : **20.02.1998**

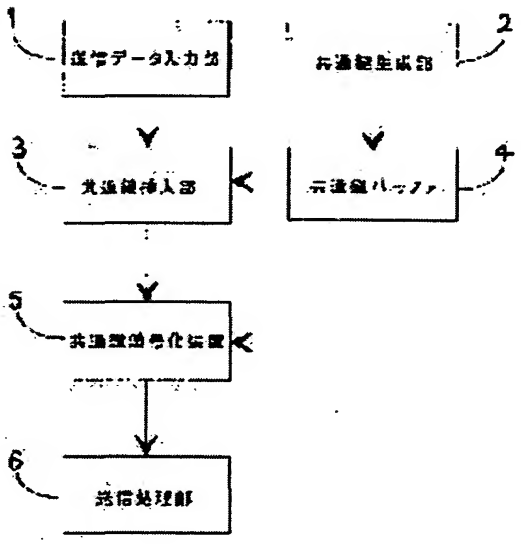
(51)Int.Cl. **H04L 9/16**
G09C 1/00
H04L 9/08

(21)Application number : **08-205528**
(22)Date of filing : **05.08.1996**

(71)Applicant : **SHARP CORP**
(72)Inventor : **AIDA WATARU**

(54) DEVICE AND METHOD FOR CIPHER COMMUNICATION

(57)Abstract:
PROBLEM TO BE SOLVED: To estimate a common key without the need to own plural common keys or secure plural common communication paths by inserting a common key to be used for a next communication into plaintext data to be sent and then ciphering and transmitting them.
SOLUTION: A common ciphering device 5 consists of a common key ciphering system such as DES and FEAL and ciphers a plaintext from a transmit data input part 1 with a currently used common key. Here, a common key generation part 2 is equipped with a random number generating device, etc., and generates a common key to be used for a next communication at random and stores it in a buffer 4. A common key insertion part 3 divides the common key in the buffer 4, and decentralizes and inserts it into the plaintext to be sent. The division size of the common key, the division size of the transmit data, and the decentralized insertion position of the common key are predetermined between communicating persons and at the time of reception, the receive data and common key to be used next are separated from the deciphered receive plaintext, but this need not be kept secret specially.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開平10－51440
(43)公開日　平成10年(1998)２月20日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/16			Ｈ０４Ｌ	9/00	６４３
Ｇ０９Ｃ	1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６３０Ｃ
			7259－5Ｊ			６３０Ｅ
Ｈ０４Ｌ	9/08			Ｈ０４Ｌ	9/00	６０１Ｅ
						６０１Ｃ

審査請求　未請求　請求項の数３　ＯＬ　（全６頁）

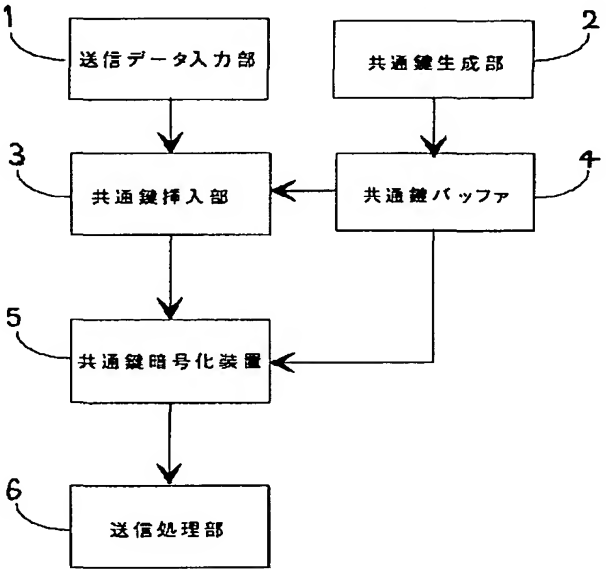
(21)出願番号　特願平8－205528

(22)出願日　平成８年(1996)８月５日

(71)出願人　000005049
シャープ株式会社
大阪府大阪市阿倍野区長池町22番22号
(72)発明者　合田　亙
大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内
(74)代理人　弁理士　梅田　勝

(54)【発明の名称】　暗号通信装置及び暗号通信方法

(57)【要約】
【課題】　本発明は、事前に複数個の共通鍵を所有する必要や複数の通信経路を確保する必要がなく、容易に共通鍵の変更を可能として、通信相手以外の者が共通鍵を推定することをより困難にする暗号通信装置及び暗号通信方法を提供することを目的とする。
【解決手段】　所定のタイミングで共通鍵を共通鍵を変更して暗号通信を行う暗号通信装置において、送信データを入力す送信データ入力部１と、次回の通信時に用いられる変更すべき共通鍵を生成する共通鍵生成部２と、送信データ入力部１にて入力された送信データに共通鍵生成部２にて生成された共通鍵を挿入する共通鍵挿入部３と、共通鍵挿入部３にて共通鍵が挿入された送信データの暗号化を行う共通鍵暗号化装置５と、共通鍵暗号化装置５にて暗号化された暗号文の送信を行う送信処理部６とから構成する。



【特許請求の範囲】

【請求項１】　所定のタイミングで共通鍵を共通鍵を変更して暗号通信を行う暗号通信装置において、
送信データを入力する送信データ入力部と、次回の通信時に用いられる変更すべき共通鍵を生成する共通鍵生成部と、前記送信データ入力部にて入力された送信データに前記共通鍵生成部にて生成された共通鍵を挿入する共通鍵挿入部と、該共通鍵挿入部にて共通鍵が挿入された送信データの暗号化を行う共通鍵暗号化装置と、該共通鍵暗号化装置にて暗号化された暗号文の送信を行う送信処理部とから構成されることを特徴とする暗号通信装置。

【請求項２】　所定のタイミングで共通鍵を共通鍵を変更して暗号通信を行う暗号通信装置において、
暗号文の受信を行う受信処理部と、該受信処理部にて受信された暗号文の復号化を行う共通鍵復号化装置と、該共通鍵暗号化装置にて復号化されたデータから受信データと次回の通信時に用いられる変更すべき共通鍵との分離を行う共通鍵分離部と、該共通鍵分離部にて分離された受信データの出力を行う受信データ出力部とから構成されることを特徴とする暗号通信装置。

【請求項３】　所定のタイミングで共通鍵を共通鍵を変更して暗号通信を行う暗号通信方法において、
送信側では次回の通信時に用いられる変更する共通鍵を送信するデータに挿入し暗号化して送信し、受信側では復号化した受信データよりデータと次回の通信時に変更する共通鍵を分離しその分離した共通鍵を次回の通信時の受信復号化に使用することを特徴とする暗号通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ディジタルデータ等の通信データを、共通鍵暗号方式にて暗号化したデータを通信する暗号通信装置及び暗号通信方法に関するものである。

【０００２】

【従来の技術】従来より、通信するデータの秘密を保持するために、その内容を暗号化することが行われている。その方法として、ＤＥＳに代表される共通鍵暗号方式と、ＲＳＡに代表される公開鍵方式とがある。公開鍵方式は、鍵を一般に公開できることから、データ暗号はもとよりディジタル署名等に用いることが可能であるが、スピードが共通鍵方式に比べるとはるかに遅い。このことから、データの暗号化には、共通鍵方式を用いることが一般的である。

【０００３】共通鍵方式では、大きなファイルや文章を暗号化する際に、平文はある固定長のブロックに分割され、通常それらの分割されたブロックのそれぞれに対して、同一の共通鍵で暗号化される。しかしながら、この暗号化されたブロックが通信相手以外の解読者に入手されると、すべての共通鍵の場合を検証することにより、共通鍵が推定されたり、ファイルや文章の統計的性質を元に共通鍵が推定されるおそれがある。

【０００４】このような暗号解読を防ぐ技術として、その一つが、特開平７－２８４０７号公報に開示されている。これによれば、送信データとは無関係でランダムなデータを送信データに挿入しておくことによって、ファイルや文章の統計的な性質を元にした暗号解読を防止できるというものである。

【０００５】また、別の暗号解読防止の技術としては、通信相手以外の解読者に共通鍵を推定される前に、共通鍵を変更するというものも有用である。

【０００６】

【発明が解決しようとする課題】しかしながら、上記特開平７－２８４０７号公報に記載の従来技術では、共通鍵を同時に同一の通信路で送信するので、共通鍵を解読されるおそれが全くないというわけではなく、十分な機密性を維持できなかった。

【０００７】一方、通信相手以外の解読者に共通鍵を推定される前に共通鍵を変更するという上記の従来技術では、何らかの形で変更されるべき共通鍵を通信相手に渡す必要があった。ところが、鍵そのものを、裸の形で同じデータ通信路を使って同時に送信することはできないので、事前に通信相手同士で複数の鍵を所有しておき、ある周期で変更するか、データ通信路とは異なるを通信路、例えば電話、ＦＡＸ等を用いて鍵の変更を通知しなければならなかった。したがって、事前に複数個の鍵を所有するための記憶部を設けるか、複数の通信経路を確保しなければならず、コストの増大を招くという問題点があった。

【０００８】本発明は、上記のような課題を解決するためになされたものであって、事前に複数個の共通鍵を所有する必要や複数の通信経路を確保する必要がなく、容易に共通鍵の変更を可能として、通信相手以外の者が共通鍵を推定することをより困難にする暗号通信装置及び暗号通信方法を提供することを目的とする。

【０００９】

【課題を解決するための手段】上記課題を解決するため、本発明では、所定のタイミングで共通鍵を共通鍵を変更して暗号通信を行う暗号通信装置において、送信データを入力す送信データ入力部と、次回の通信時に用いられる変更すべき共通鍵を生成する共通鍵生成部と、送信データ入力部にて入力された送信データに共通鍵生成部にて生成された共通鍵を挿入する共通鍵挿入部と、その共通鍵挿入部にて共通鍵が挿入された送信データの暗号化を行う共通鍵暗号化装置と、その共通鍵暗号化装置にて暗号化された暗号文の送信を行う送信処理部とから構成している。

【００１０】また、本発明では、所定のタイミングで共通鍵を共通鍵を変更して暗号通信を行う暗号通信装置に

おいて、暗号文の受信を行う受信処理部と、その受信処理部にて受信された暗号文の復号化を行う共通鍵復号化装置と、その共通鍵暗号化装置にて復号化されたデータから受信データと次回の通信時に用いられる変更すべき共通鍵との分離を行う共通鍵分離部と、その共通鍵分離部にて分離された受信データの出力を行う受信データ出力部とから構成している。

【００１１】また、本発明では、所定のタイミングで共通鍵を共通鍵を変更して暗号通信を行う暗号通信方法において、送信側では次回の通信時に用いられる変更する共通鍵を送信するデータに挿入し暗号化して送信し、受信側では復号化した受信データよりデータと次回の通信時に変更する共通鍵を分離しその分離した共通鍵を次回の通信時の受信復号化に使用することとしている。

【００１２】

【発明の実施の形態】以下、本発明による一実施形態について、図面を参照して説明する。図１は、本発明による実施形態である送信側の暗号通信装置のブロック図を示す。図１に示すように、この暗号通信装置は、送信データを入力す送信データ入力部１、次回の通信時に用いられる変更すべき共通鍵を生成する共通鍵生成部２、共通鍵生成部２にて生成された変更すべき共通鍵を保持する共通鍵バッファ４、送信データ入力部１にて入力された送信データである平文に、共通鍵生成部２にて生成された共通鍵を挿入する共通鍵挿入部３、共通鍵挿入部３にて共通鍵が挿入された送信平文の暗号化を行う共通鍵暗号化装置５、共通鍵暗号化装置５にて暗号化された暗号文の送信を行う送信処理部６から構成されるものである。

【００１３】この暗号通信装置の共通鍵挿入部３においては、実際に送信する文章やファイルの所定位置に、共通鍵生成部２にて生成された変更すべき共通鍵の所定サイズを挿入する。これら送信データの分割サイズ、及び変更するべき共通鍵の分割サイズを、通信者同士で事前に打ち合わせておくが、これらの値は特に秘密にしておく必要はない。さらに、その値に対しても特に制限はなく、共通鍵暗号化装置５におけるブロックサイズと無関係に定めてもよい。ただし、暗号文は送信データと無関係でランダムな共通鍵が挿入された形式とすることが望ましく、その際にそのランダム度を上げるために、送信データの区切りサイズを共通鍵暗号化装置５におけるブロックサイズよりも小さい値とすることが望ましい。

【００１４】共通鍵挿入部３にて挿入される変更するべき共通鍵は共通鍵生成部２で生成されるものであり、乱数発生装置などを用いて、ランダムな共通鍵データの生成が実現される。そして、生成されるそのデータサイズは、あらかじめ取り決められた共通鍵分割サイズの倍数で、かつ共通鍵暗号化装置５の共通鍵サイズを超える値の最小値である。また、後述の受信側では、共通鍵サイズを超えているデータは無視される。

【００１５】図２は、共通鍵挿入部３における送信データの変化の様子を示した説明図である。図２において、上段の送信データ１０は、送信データ入力部１にて入力されるデータ、即ち実際に受信側とやり取りを行うデータを示す。そして、共通鍵Ｋ１（１３），Ｋ２（１４），・・・は上記の共通鍵生成部２にて生成されるものであり、図２中で実線が共通鍵暗号化装置５にて用いられる鍵サイズを表し、点線が共通鍵生成部２にて生成されるサイズを表している。なお、生成サイズと鍵サイズとの差に相当するデータは、後述の受信側の共通鍵復号化装置において無視されるものである。

【００１６】また、送信データ１０及び挿入される共通鍵１２は、共通鍵挿入部３において混合され、その結果、図２の中段の暗号化装置に入力される平文１１のようになり、共通鍵暗号化装置５に入力される。なお、平文１１のＰ１，Ｐ２，Ｐ３は共通鍵暗号化装置５のブロック化サイズを表しており、これらは共通鍵暗号化装置５に順次Ｐ１，Ｐ２，Ｐ３の順に入力されることになる。

【００１７】共通鍵暗号化装置５は、ＤＥＳやＦＥＡＬなどの共通鍵暗号方式により構成されるものであり、現在用いられている共通鍵を用いて暗号化される。なお、共通鍵の初期値を、通信者同士であらかじめ打ち合わせておく必要があり、これは秘密にしておく必要がある。そして、ここで暗号化された暗号文は、送信処理部６にて送信される。

【００１８】次に、本発明による実施形態である受信側の暗号通信装置について、そのブロック図である図３を用いて説明する。図３に示すように、この暗号通信装置は、暗号文の受信を行う受信処理部２６、受信処理部２６にて受信された暗号文の復号化を行う共通鍵復号化装置２５、共通鍵暗号化装置２５にて復号化されたデータから受信データと次回の通信時に用いられる変更すべき共通鍵との分離を行う共通鍵分離部２３、共通鍵分離部２３にて分離された変更すべき共通鍵を保持しておく共通鍵バッファ２４、共通鍵分離部２３にて分離された受信データの出力を行う受信データ出力部２１から構成される。

【００１９】この通信装置の受信処理部２６において通信相手からの暗号文を受信した後、共通鍵復号化装置２５では、現在用いられている共通鍵に基づいて受信暗号文を復号化する。そして、共通鍵分離部２３では、通信者同士であらかじめ打ち合わせている受信データの分割サイズと変更すべき共通鍵の分割サイズとから、復号化された受信平文を、受信データと変更すべき共通鍵とを分離する。これは、前述の図２における送信データに、共通鍵を挿入する過程の全く逆の流れになる。

【００２０】そして、分離された受信データが受信データ出力部２１に出力される一方、分離された共通鍵が共通鍵バッファ２４に保持される。ここで、通信者同士で

あらかじめ打ち合わせている共通鍵分離サイズと共通鍵サイズとによるが、通常は一度に共通鍵サイズ分のデータが送信されることはなく、分割されて送信されるので、共通鍵のサイズ分のデータが受信されるまで、共通鍵バッファ２４に追加していく。また、共通鍵分離サイズにっよては、共通鍵復号化装置２５で用いられる共通鍵サイズを超えることがあるが、超えた分は無視され、共通鍵として有効なデータとならない。

【００２１】次に、共通鍵が変更される様子について説明する。まず、送信側では、１つの共通鍵データに対して、分割された共通鍵データの全てのブロックにおいて送信データへの挿入が終了した次の暗号化ブロックで、共通鍵の変更を行う。例えば、図２においては、Ｐ１，Ｐ２，Ｐ３のブロックは、共通鍵Ｋ１の一つ以前に生成された共通鍵を用いて暗号化され、Ｐ４のブロックから共通鍵Ｋ１にて暗号化される。

【００２２】一方、受信側では、分離された共通鍵が、共通鍵復号化装置２５で用いられる鍵サイズを超えた次の復号化ブロックで変更を行う。例えば、図２においては、Ｐ１～Ｐ３に相当する暗号文のブロックが共通鍵Ｋ１の一つ以前に分離された共通鍵で復号化され、Ｐ４に相当する暗号文のブロックから共通鍵Ｋ１で復号化されることになる。

【００２３】

【発明の効果】以上のように、本発明によれば、上記実施形態にて説明したような処理を繰り返して行うことにより、送信データとそれに無関係な冗長ビットを混在させ、暗号文から統計的性質を用いると共に、共通鍵解読を防止することが可能となる。さらに、複数の通信路や事前に共通鍵を保有しておく必要なく、容易に共通鍵を取り替えることが可能となり、通信相手以外の者が共通鍵を推定することがより困難となり、高い機密性を有する暗号通信装置を実現することができる。

【図面の簡単な説明】

【図１】本発明による実施形態の送信側の暗号通信装置の概略構成を示すブロック図である。

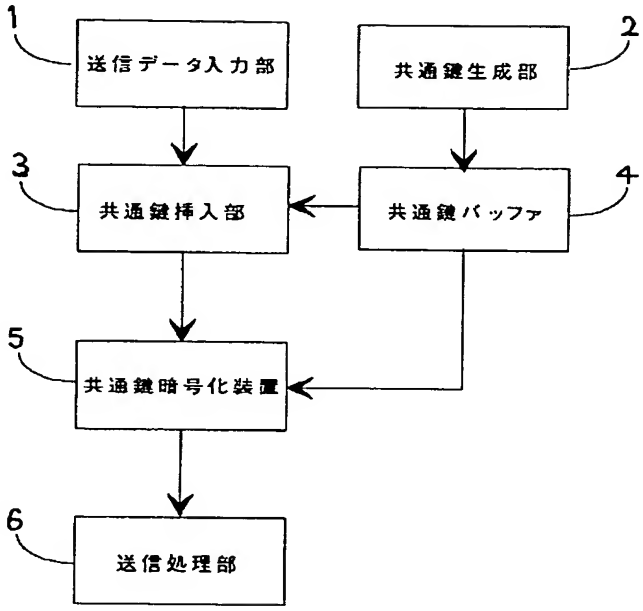
【図２】本発明による実施形態の受信側の暗号通信装置の概略構成を示すブロック図である。

【図３】送信データと共通鍵データの形式を示す図である。

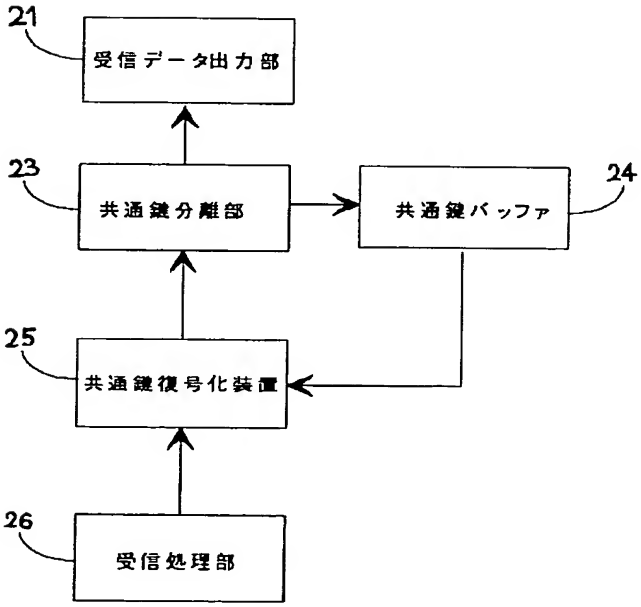
【符号の説明】

１　送信データ入力部
２　共通鍵生成部
３　共通鍵挿入部
４　共通鍵バッファ
５　共通鍵暗号化装置
６　送信処理部
１０　送信データ
１１　暗号化装置に入力される平文
１２　挿入される共通鍵
２１　受信データ出力部
２３　共通鍵分離部
２４　共通鍵バッファ
２５　共通鍵復号化装置
２６　受信処理部

【図１】



【図３】



【図２】